

# Linear Programming Tools for Analyzing Strategic Games of Independence-Friendly Logic and Applications

Merlijn Sevenster

January 21, 2014

## Abstract

In recent work, semantic games of independence-friendly logic were studied in strategic form in terms of (mixed strategy) Nash equilibria. The class of strategic games of independence-friendly logic is contained in the class of win-loss, zero-sum two-player games. In this note we draw on the theory of linear programming to develop tools to analyze the value of such games. We give two applications of these tools to independence-friendly logic under the so-called equilibrium semantics.

## 1 Introduction

At the heart of game-theoretic semantics [7, 8] lies the understanding that meaning emerges as the result of the interaction between rational agents who act in their own interest according to a set of rules. The meaning that arises thus is attached to the linguistic expression that constitutes this set of rules. The concept of game was used to flesh out this understanding, a concept that was also applied by Wittgenstein to the philosophy of (natural) language [16]. A sample game, well known in the context of independence-friendly logic, is defined by the following set of rules parameterized by a function  $f$ . First an opponent chooses an  $x$  and  $\varepsilon > 0$  on the reals. Then we choose a  $\delta > 0$  independent of  $x$ . The interaction terminates after the opponent has chosen a  $y$ . We “win” if the series of objects satisfies the condition

$$|x - y| < \delta \text{ implies } |f(x) - f(y)| < \varepsilon, \quad (1)$$

otherwise the opponent “wins”.

The linguistic expression of this rule set, in the syntax of independence-friendly (IF) logic, is

$$\forall x \forall \varepsilon (\exists \delta / x) \forall y \psi(x, \varepsilon, \delta, y),$$

where  $\psi(x, \varepsilon, \delta, y)$  is a formalization of (1). In game-theoretic semantics, the meaning of the latter expression, or any IF sentence for that matter,

is defined as the conditions under which we win the game. We will make this more precise in due course.

For now it is important to emphasize that game-theoretic semantics puts rule-governed interaction at the center of attention, and that meaning is derived from it. This view must be contrasted to the view according to which the meaning of a logical expression is determined by conditions under which it is “true” in a (formalized) state of affairs. It seems that Tarski semantics for first-order logic is a formal counterpart of this view.

Interaction between self-interested agents is studied in game theory. In this area, a (*pure*) *strategy* for a player completely specifies how to move in each choice point for that player. If we are given one strategy of each player in a game (in the formal, game-theoretic sense of the word), then we can traverse the sequence of choice points that arise if we follow the moving player’s strategy. The respective players’ *payoffs* are distributed among the players once the terminal node in this sequence is reached. A win-loss game is a game in which the players can either win (i.e., receive payoff 1) or lose (i.e., receive 0). In the context of a win-loss game, a strategy is *winning* if it results in a win for its owner against each strategy of its opponent.

Game-theoretic semantics for independence-friendly logic was developed (first in spirit [9], then in formalism [3]) in the framework of extensive games. This framework considers a game as a *game tree* in which each node corresponds to a choice point for a player or a terminal node (i.e., a node in which payoff is returned to the players). Folklore has it that semantic games of IF logic are played between Eloise and Abelard. The game tree that formalizes the interactions between Eloise and Abelard constituting the meaning of an IF sentence  $\phi$  in the context of a suitable structure  $\mathbb{M}$  is called an *extensive game of imperfect information*, denoted  $G(\mathbb{M}, \phi)$ .

The meaning of  $\phi$  can be seen to emerge from interaction in  $G(\mathbb{M}, \phi)$ , by inspecting that the condition

$$\phi \text{ is true on } \mathbb{M} \text{ (written } \mathbb{M} \models^+ \phi) \quad (2)$$

coincides with the condition

$$\text{Eloise has a winning strategy in the game } G(\mathbb{M}, \phi), \quad (3)$$

and that

$$\phi \text{ is false on } \mathbb{M} \text{ (written } \mathbb{M} \models^- \phi) \quad (4)$$

coincides with

$$\text{Abelard has a winning strategy in the game } G(\mathbb{M}, \phi). \quad (5)$$

From a logical point of view, game-theoretic semantics has several advantages. Its tree-based view nicely reflects the dependence between nested quantifiers. Conditions (2) to (5) show us how one particular type of interaction coincides with the meaning of IF sentences, at least in terms of their truth and falsity conditions.

The equivalences between Conditions (2) to (5) show us how known grounds — i.e., the Tarskian notions of truth and falsity — can be covered

by game-theoretical semantics. They also give us a lead for exploring uncharted territory. Namely, we see that the above conditions are based on one mode of interaction only, that is, one player having a winning strategy. Thus a whole research agenda unfolds itself in front of us: analyzing the interrelations between game-theoretic interactions on the one hand and the meanings that arise from them on the other hand. The Matching Pennies sentence  $\phi_{\text{MP}}$  serves to illustrate the type of questions that motivate this agenda:

$$\forall x(\exists y/x)x = y$$

On structures  $\mathbb{M}$  with more than one element, neither player has a winning strategy in the game  $G(\mathbb{M}, \phi_{\text{MP}})$ . Such games are said to be *undetermined*. The games  $G(\mathbb{M}, \phi_{\text{MP}})$  are not covered by the Conditions (3) and (5), as if no meaning can be seen to emerge from them.

This observation can be made more precise. Every IF sentence  $\phi$  partitions the class of suitable structures in three:

$$(\llbracket \phi \rrbracket^-, \llbracket \phi \rrbracket^\#, \llbracket \phi \rrbracket^+),$$

where  $\llbracket \phi \rrbracket^+$  denotes the set of structures on which Eloise has a winning strategy,  $\llbracket \phi \rrbracket^-$  denotes the set of structures on which Abelard has a winning strategy, and  $\llbracket \phi \rrbracket^\#$  contains the other structures, i.e., the structures on which neither player has a winning strategy. In the case of the Matching Pennies sentence,  $\llbracket \phi_{\text{MP}} \rrbracket^+$  is the set of structures with one element;  $\llbracket \phi_{\text{MP}} \rrbracket^-$  is empty; and  $\llbracket \phi_{\text{MP}} \rrbracket^\#$  is the set of structures with more than one element. The observation that game-theoretic semantics does not cover the undetermined games of  $\phi_{\text{MP}}$ , i.e. the games on  $\llbracket \phi_{\text{MP}} \rrbracket^\#$ , touches on the following question: How can we give a *direct* definition of  $\llbracket \phi \rrbracket^\#$ ? — understanding that its present definition, stated in terms of the absence of a winning strategy for either player, is indirect.

We can also study the class of semantic games as a game-theoretic entity in its own right and ignore the fact that each game in this class is constituted by an IF sentence and a structure. From such a point of view, it is only natural<sup>1</sup> to generalize from pure strategies to *mixed strategies*, those being the dominant species of strategies in game theory. Mixed strategies are studied more naturally in the framework of *strategic games*, which ignore the games' sequential turn-taking dynamics. Finally, instead of studying winning (pure) strategies, we can now shift our attention to equilibrium mixed strategies, that is, mixed strategies that cannot be improved upon by any of the players.

In a recent publication [14], rooted in an observation by Ajtai [1] and anticipated in [13, 5], the strategic game theory of IF games was developed. A mixed strategy is a probability distribution over a set of pure strategies. If Eloise and Abelard both play mixed strategies, that is, if they pick their pure strategies at random according to their mixed strategies, the pair of pure strategies that will be played is effectively selected from the lottery determined by the product of their mixed strategies. If we associate payoff 0 with Eloise losing the outcome of playing two pure strategies against each other, and 1 with her winning, we can define the *expected payoff* of

---

<sup>1</sup>The author is grateful to Allen L. Mann for suggesting this point of view.

Eloise as the expected utility that is returned to her in this lottery. It is not hard to see that Eloise's expected utility falls in  $[0, 1]$ .

Informally, an equilibrium is a state of the game in which the players' powers to influence the outcome are in balance, or, somewhat more formally, it is a pair of mixed strategies in which neither player can benefit from unilateral deviation. The *value* of a strategic game between Eloise and Abelard is defined as Eloise's expected utility of an equilibrium.

In [14], the strategic IF game  $\Gamma(\mathbb{M}, \phi)$  was defined as the strategic counterpart of the extensive game  $G(\mathbb{M}, \phi)$ . It was further postulated that the *value* of  $\phi$  on  $\mathbb{M}$  is the value of  $\Gamma(\mathbb{M}, \phi)$ , that is, Eloise's *expected utility* in  $\Gamma(\mathbb{M}, \phi)$ . For instance, as is easily proven (see also Example 6 below), the Matching Pennies sentence has value  $1/n$  on structures of size  $n$ . The notation  $\mathbb{M} \models_{\varepsilon} \phi$  was introduced to indicate that  $\phi$  has value  $\varepsilon$  on  $\mathbb{M}$ . We will introduce the framework of *equilibrium semantics* and key results more rigorously in the next section, including the results by which every finite strategic IF game has one unique value.

The strategic view disregards the sequential turn-taking of the games trees, which are so nicely reflected the quantifier alternation of IF sentences. In return we get a formalism in which the notion of strategy is atomic. This somehow matches the way in which interaction is primitive in the philosophy behind game-theoretic semantics. Furthermore, it is to be understood that the strategic view on semantic games is a generalization of the extensive view, in the sense that conditions can be found in terms of equilibrium mixed strategies that are equivalent to Conditions 2 and 5. Indeed, one of the first results about equilibrium semantics, reiterated in the next section, has it that

$$[\phi]^{-} = [\phi]^0 \quad (6)$$

$$[\phi]^{+} = [\phi]^1, \quad (7)$$

where  $[\phi]^{\varepsilon}$  denotes the class of structures on which  $\phi$  has value  $\varepsilon$ . This result shows that equilibrium semantics is a *conservative extension* of traditional game-theoretic semantics. It also shows that  $[\phi]^{\#}$ , which was defined indirectly in game-theoretic semantics, can be defined directly in equilibrium semantics:

$$[\phi]^{\#} = \bigcup_{\varepsilon \in (0,1)} [\phi]^{\varepsilon}. \quad (8)$$

It is yet to be seen what type of meaning is constituted by the interaction studied in equilibrium semantics. At present, no coherent semantic interpretation has been given of very the notion of value. In an attempt to get a handle on the problem of interpreting  $\models_{\varepsilon}$  consider the partitioning

$$([\phi]^{\varepsilon})_{\varepsilon \in [0,1]}$$

for any IF sentence  $\phi$ . For instance,  $[\phi_{\text{MP}}]^{1/n}$  contains the structures of size  $n$ . With each class  $[\phi]^{\varepsilon}$  we can seek a logical expression  $\psi^{\varepsilon}$  that defines it, in the sense that  $\mathbb{M} \in [\phi]^{\varepsilon}$  if, and only if,  $\psi^{\varepsilon}$  is true on  $\mathbb{M}$ . From a model-theoretic point of view we are interested in the logical languages

in which such  $\psi$  can be defined, whereas, from a more philosophical viewpoint, we are interested to learn the interrelations between the sentences in

$$(\psi^\varepsilon)_{\varepsilon \in [0,1]}.$$

For instance, how does  $\psi^\varepsilon$  relate to  $\psi^1$ , which expresses  $\phi$ 's truth conditions, and  $\psi^0$ , which expresses its falsity conditions?

One of the obstacles we are facing in this respect is the informal way of thinking about game-theoretical semantics. For instance, we grew used to thinking of Eloise “wanting” to prove that the sentence  $\phi$  is true, and Abelard “wanting” to prove that it is false. In the case of the Matching Pennies sentence, this would mean that Eloise wants to establish that the structure has one element and that Abelard wants to establish the logical contradiction, whatever that may mean.

In equilibrium semantics, it is unclear what semantic relation Eloise and Abelard want to establish between  $\phi$  and  $\mathbb{M}$ . For all we know, Eloise and Abelard want to maximize their payoff in  $\Gamma(\mathbb{M}, \phi)$ , but what does that tell us about the relation between  $\phi$  and  $\mathbb{M}$ ?

Another obstacle for understanding  $\models_\varepsilon$  is the fact that we lack tools to analyze strategic IF games. Establishing the series  $(\psi^\varepsilon)_{\varepsilon \in [0,1]}$  of seemingly simple  $\phi$  may take several pages of text, especially if  $\phi$  is interpreted on arbitrary graph-like structures. To grasp this point it is instructive to realize that the problem of determining the value of an arbitrary win/loss game with values 0 and 1 reduces to the problem of determining the value of  $\forall x(\exists y/x)R(x, y)$ , in the sense that if we have an algorithm to solve the latter, we can tweak it to solve the former.

This computational concern touches on the worst-case computational complexity of determining the value of an arbitrary win/loss game. It is known that this problem can be defined as a linear programming problem, for which efficient (polynomial time) algorithms have been proposed. Unfortunately, these algorithm are fairly intricate, which as yet renders them quite useless, in their current forms, for establishing the value of strategic IF games.

In this paper, we shall exploit the linear programming view on strategic IF games to develop a set of tools for determining and approximating their value. It is important to realize that the tools developed in this way are weaker than the efficient algorithms that were proposed earlier to solve arbitrary linear programming problem. If our results have any merits, it may be in the fact that they help us to more easily determine the value of certain strategic IF games, or that they inspire the construction of more powerful tools.

In the next section, we will review definitions and elementary results of equilibriums semantics. In Section 3 we present some tools to analyze win-loss, zero-sum, two-player strategic game. In Section 4 we apply these tools to analyze the values of two IF sentences that pertain to the birthday problem and hashing.

## 2 Preliminaries

An extensive game  $G$  describes all positions of the game and how it proceeds from one to the other. In an extensive game with players  $P$ , each player  $p \in P$  has a set of (*pure*) *strategies*  $S_p$ . A pure strategy is essentially a rule book that prescribes how its owner moves in every position of the game (i.e., *history*) in which it is his/her turn. A definition of extensive games can be found in [3, 10].

A *strategy profile* (for the players  $P$ )  $\bar{\sigma}$  is a function that selects an appropriate strategy for each player in  $P$ . If  $P = \{p_0, \dots, p_{n-1}\}$  we shall also write  $\bar{\sigma}$  as the sequence  $(\sigma_{p_0}, \dots, \sigma_{p_{n-1}})$ . An extensive game  $G$  has a utility function  $u_p$  for each player  $p$  that assigns a real value to each of the game's strategy profiles.

We shall be interested in two-player games, so that our strategy profiles contain two strategies. We shall use the symbols  $\exists$  and  $\forall$  to mark the game's contestants, Eloise and Abelard:  $P = \{\exists, \forall\}$ . Moreover we shall focus on *win-loss* and *zero-sum* games, that is, the utility functions  $u_\exists$  and  $u_\forall$  will be functions with range  $\{0, 1\}$  such that for each strategy profile  $(\sigma, \tau)$ ,  $u_\exists(\sigma, \tau) + u_\forall(\sigma, \tau) = 1$ . Since in this type of games,  $u_\forall$  is uniquely determined by  $u_\exists$ , we shall simply write  $u$  for  $u_\exists$  and mostly ignore  $u_\forall$ .

A pure strategy  $\sigma \in S_p$  is *winning* in a win-loss, zero-sum game if  $u_p(\sigma, \tau) = 1$  for each strategy  $\tau$  of  $p$ 's opponent  $\bar{p}$ .

Independence-friendly logic is the extension of first-order logic whose quantifiers ( $Qx/X$ ) are furnished with sets of variables  $X$  indicating that the choice of quantifier  $Qx$  be made independent from the variables in  $X$ . In this paper we shall only use the syntax of IF logic when we apply our game-theoretic results to express certain properties. We refer the reader to [10] for a comprehensive introduction to the field of IF logic, which also introduces more gently the basic notions of equilibrium semantics.

Sentences of IF logic are evaluated on *structures*

$$\mathbb{M} = (M, R_0^{\mathbb{M}}, R_1^{\mathbb{M}}, \dots, f_0^{\mathbb{M}}, f_1^{\mathbb{M}}, \dots),$$

where  $M$  is the *universe* of  $\mathbb{M}$ ,  $R_i^{\mathbb{M}}$  is the *interpretation* of *relation symbol*  $R_i$  and  $f_i^{\mathbb{M}}$  is the interpretation of *function symbol*  $f_i$ , as usual.

The semantic game of an IF sentence  $\phi$  on a structure  $\mathbb{M}$  gives rise to the (*extensive*) *IF game*  $G(\mathbb{M}, \phi)$ , which is a two-player, win-loss and zero-sum game. It is also a game of imperfect information if  $\phi$  has quantifiers ( $Qx/X$ ) in which  $X$  is nonempty.

The framework of strategic game theory gives another way of looking at games. Suppose that  $G$  is the extensive formalization of a game. Then, the strategic form of the same game would be

$$\Gamma = ((S_p)_{p \in P}, (u_p)_{p \in P}),$$

where  $P$  is the set of players as before,  $S_p$  is the set of  $p$ 's pure strategies in  $G$ , and  $u_p$  is player  $p$ 's utility function in  $G$ . The strategic game  $\Gamma$  is two-player/win-loss/zero-sum, whenever  $G$  is. We shall write  $\Gamma(\mathbb{M}, \phi)$  for the *strategic IF game* that is the strategic counterpart of the extensive IF game  $G(\mathbb{M}, \phi)$ .

A *mixed strategy*  $\mu_p$  of player  $p$  in  $\Gamma$  is a probability distribution over  $S_p$ , that is,  $\mu_p$  is a function for which for every  $\sigma \in S_p$ ,  $0 \leq \mu_p(\sigma) \leq 1$ , and  $\sum_{\sigma \in S_p} \mu_p(\sigma) = 1$ . The mixed strategy  $\mu_p$  is *uniform* if it assigns equal probability to each pure strategy in  $S_p$ . We say that  $\mu_p$  is *uniform in  $T$* , for any  $T \subseteq S_p$ , if the domain of  $\mu_p$  is  $T$  and if it assigns equal probability to each pure strategy in  $T$ .

We extend the notion of strategy profile to mixed strategies; whence a strategy profile may also refer to a sequence  $(\mu_p)_{p \in P}$  of mixed strategies. A strategy profile of mixed strategies defines a *lottery* over the set of outcomes of the game, that is, strategy profile  $(\sigma_p)_{p \in P}$  is drawn with likelihood

$$\prod_{p \in P} \mu_p(\sigma_p).$$

The *expected utility* for player  $p$  is given by  $p$ 's expected utility in the lottery. For a strategy profile of mixed strategies  $(\mu_{\exists}, \mu_{\forall})$ , the expected utility is defined as as

$$U_p(\mu_{\exists}, \mu_{\forall}) = \sum_{\sigma \in S_{\exists}} \sum_{\tau \in S_{\forall}} \mu_{\exists}(\sigma) \mu_{\forall}(\tau) u_p(\sigma, \tau).$$

If  $\Gamma$  is a zero-sum and win-loss game between  $\exists$  and  $\forall$ , then we have that  $U_{\exists}(\mu, \nu) + U_{\forall}(\mu, \nu) = 1$ . In this case, for the same reason as before, we shall write  $U$  for  $U_{\exists}$  and forget about  $U_{\forall}$ .

The theory of mixed strategy equilibrium predicts that Eloise and Abelard will settle on a pair of mixed strategies in which neither player benefits from unilateral deviation, that is, from choosing another mixed strategy.

**Definition 1.** *Let  $\Gamma$  be a two-player strategic game. The strategy profile  $(\mu_{\exists}, \mu_{\forall})$  is an equilibrium (in mixed strategies) in  $\Gamma$  if for each player  $p \in \{\exists, \forall\}$ ,*

$$U_p(\mu_p, \mu_{\bar{p}}) \geq U_p(\mu'_p, \mu_{\bar{p}})$$

for each mixed strategy  $\mu'_p$  of  $p$ .

A strategy in an equilibrium is called an equilibrium strategy.

The Minimax Theorem (see Theorem 2 below) shows that every finite, two-player, zero-sum game  $\Gamma$  has an equilibrium. Nash [11] later generalized this result to arbitrary finite strategic games, and this type of equilibrium has henceforth been associated with his name. Since in this work we shall only require the Minimax Theorem, we shall not use the term Nash equilibrium despite the fact that it seems to be more common in the literature on game theory.

It is not hard to see that if  $\Gamma$  has multiple equilibria, they all return the same expected utility to Eloise. We call this the *value* of the game, and write it as  $\mathcal{V}(\Gamma)$ . We define *equilibrium semantics* as the relation  $\models_{\varepsilon}$  for which

$$\mathbb{M} \models_{\varepsilon} \phi \quad \text{iff} \quad \mathcal{V}(\Gamma) = \varepsilon,$$

where  $\Gamma = \Gamma(\mathbb{M}, \phi)$ . This relation is well defined for finite structures  $\mathbb{M}$ , but not necessarily on infinite structures. Thus, in this paper, we shall only consider finite structures.

The present definition of equilibrium semantics is not compositional, that is, the value of an IF formula is not determined on the basis of the values of its subformulas. Interestingly, it was shown by Galliani and Mann [6] that compositionality can be restored by extending Hodges' trump semantics with probability distributions over assignments. This approach may yield other tools for analyzing the values of IF strategic games.

### 3 Games

In this section we take a linear programming perspective on computing the value of two-person, zero-sum strategic games that is known from the literature [12]. This class of games contains the strategic IF games as a subclass. Thus we can use insights obtained to construct tools for computing and approximating the value of strategic IF games.

#### 3.1 Linear programming

We write  $0, \dots, m-1$  for Eloise's pure strategies and  $0, \dots, n-1$  for Abelard's in a strategic game. If Eloise plays  $i$  and Abelard plays  $j$ , Eloise receives  $u(i, j) \in \{0, 1\}$ . Oftentimes we shall consider the payoff function  $u$  as a matrix:

$$\begin{bmatrix} u(0, 0) & \cdots & u(0, n-1) \\ \vdots & \ddots & \vdots \\ u(m-1, 0) & \cdots & u(m-1, n-1) \end{bmatrix}$$

In fact we shall regard such matrices  $u$  as games in their own right, understanding that Eloise controls the row strategies and Abelard controls the column strategies. Accordingly we write  $\mathcal{V}(u)$  for the value of the game corresponding to the matrix  $u$ . *Throughout this section the word "game" designates any matrix  $u$  with entries carrying values in the range  $\{0, 1\}$ , unless specified otherwise.*

The *security level for Eloise* in a game  $u$  is defined as

$$\max_{\mu} \min_{\nu} U(\mu, \nu),$$

where  $\mu$  ranges over Eloise's mixed strategies in  $u$  and  $\nu$  over Abelard's. It may be instructive to take a game-theoretic view on the expression  $\max_{\mu} \min_{\nu} U(\mu, \nu)$ . According to this view, the security level is the value that is the result of a game between Maximizer and Minimizer. In this game, Maximizer chooses a mixed strategy  $\mu$  for  $\max_{\mu}$ . Then Minimizer chooses a mixed strategy  $\nu$  for  $\min_{\nu}$  knowing  $\mu$ . The game ends and Maximizer receives  $U(\mu, \nu)$  and Minimizer receives  $1 - U(\mu, \nu)$ . Thus the security level corresponds to the maximal value that Maximizer can secure. Similarly, the *security level for Abelard* is defined as  $\min_{\nu} \max_{\mu} U(\mu, \nu)$ .

Note the informational asymmetry between the games defined by

$$\max_{\mu} \min_{\nu} U(\mu, \nu)$$



and

$$\min_{\nu} \max_{\mu} U(\mu, \nu).$$

In the former game Minimizer observes the move by Maximizer before she picks her mixed strategy, whereas in the latter game Maximizer has the informational advantage. Below we shall associate Maximizer with Eloise and Minimizer with Abelard.

Von Neumann's Minimax Theorem [15] compares the players' security levels with each other and with the game's value.

**Theorem 2** (Minimax). *For every zero-sum, two-player game  $u$ ,*

1.  $\max_{\mu} \min_{\nu} U(\mu, \nu) = \min_{\nu} \max_{\mu} U(\mu, \nu)$ ; and
2.  $\mathcal{V}(u) = \max_{\mu} \min_{\nu} U(\mu, \nu)$ .

The Minimax Theorem implies that the informational asymmetry between  $\max_{\mu} \min_{\nu}$  and  $\min_{\nu} \max_{\mu}$  cannot be utilized by either player, that is, it does not negatively affect her expected utility if Eloise hands over to Abelard the strategy  $\mu$  that maximizes  $\min_{\nu} U(\mu, \nu)$  before Abelard makes his choice. In the same vein, it does not negatively affect Abelard's expected utility if he hands over the strategy  $\nu$  that minimizes  $\max_{\mu} U(\mu, \nu)$  before Eloise makes her choice.

It is easy to check that for any given mixed strategy  $\mu$ ,

$$\min_{\nu} U(\mu, \nu) = \min_{0 \leq j < n} U(\mu, j), \quad (9)$$

where  $U(\mu, j)$  denotes the expected utility of Eloise if she plays  $\mu$  against the pure strategy  $j$ . So, whenever Eloise hands over her strategy  $\mu$ , all Abelard needs to do is compute the expected utility  $U(\mu, j)$  for each of his pure strategies  $j$ . If  $\mu$  is an equilibrium strategy and  $j$  minimizes  $U(\mu, j)$ ,  $\mathcal{V}(u)$  is equal to  $U(\mu, j)$ .

Introduce the variable  $\mu_i$  to represent the value  $\mu(i)$  that Eloise's mixed strategy  $\mu$  assigns to her pure strategy  $i$ . We can regard  $\mu$  as the row vector

$$[\mu_0, \dots, \mu_{m-1}].$$

Multiplying Eloise's strategy  $\mu$  (as row vector) with  $u$  yields the row vector

$$[U(\mu, 0), \dots, U(\mu, n-1)].$$

Reading Abelard's strategy  $\nu$  as a column vector,  $\mu u \nu$  is equal to  $U(\mu, \nu)$ .

We write  $\text{Row}^u(i)$  for the  $i$ th row in  $u$ , which is a row vector, and  $\text{Col}^u(j)$  for the  $j$ th column in  $u$ , which is a column vector. For a vector of values  $v = [v_0, \dots, v_{k-1}]$ , let  $\Sigma v$  denote the sum of its elements:  $\sum_{0 \leq i < k} v_i$ . Clearly, for our  $u$ ,  $\Sigma \text{Row}^u(i)$  coincides with the number of nonzero entries in the  $i$ th row in  $u$ . We say that  $u$  is *row balanced* if all its rows have the same sum:  $\Sigma \text{Row}^u(i) = \Sigma \text{Row}^u(i')$ , for all  $0 \leq i, i' < m$ . Similarly, we say that  $u$  is *column balanced* if  $\Sigma \text{Col}^u(j) = \Sigma \text{Col}^u(j')$ , for all  $0 \leq j, j' < n$ . A game is *balanced* if it is both row and column balanced.

If Eloise plays  $\mu$  and Abelard plays  $j$ , Eloise's expected utility  $U(\mu, j)$  is the product of  $\mu$  and  $\text{Col}^u(j)$ . Consequently, Eloise's task of maximizing

$$\min_{0 \leq j < n} U(\mu, j)$$

boils down to selecting a mixed strategy  $\mu$  that maximizes the minimal element  $v$  in

$$[\mu \text{Col}^u(0), \dots, \mu \text{Col}^u(n-1)],$$

that is, optimizing  $v$  subject to the following constraints:

$$\begin{aligned} \mu \text{Col}^u(0) &\geq v \\ &\vdots \\ \mu \text{Col}^u(n-1) &\geq v, \end{aligned}$$

plus (for every  $0 \leq i < n$ ):

$$\mu_i \geq 0$$

and

$$\mu_0 + \dots + \mu_{n-1} = 1.$$

The latter  $n + 1$  constraints ensure that  $\mu$  is a proper probability distribution. Modulo some rewriting, the above constraints constitute a linear programming problem. The solution, i.e., the optimized value for  $v$ , coincides with Eloise's security level in the underlying game, which coincides with its value by the Minimax Theorem.

As an example consider the game:

$$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{bmatrix},$$

which yields the following four constraints (in addition to the five constraints that ensure that  $\mu$  is a probability distribution):

$$\begin{aligned} \mu_0 + \mu_2 + \mu_3 &\geq v \\ \mu_0 + \mu_1 + \mu_3 &\geq v \\ \mu_1 + \mu_2 + \mu_3 &\geq v \\ 0 &\geq v. \end{aligned}$$

Due to the fourth constraint, the maximum for  $v$  is 0 regardless of  $\mu_0, \dots, \mu_3$ . Thus, whatever strategy Eloise plays, she has expected utility 0, that is, Abelard has a winning strategy.

Flipping the bottom right value gives the game

$$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix},$$

yielding the same constraints as above, replacing the fourth by

$$\mu_3 \geq v.$$

The maximum value for  $v$  is 1, realized by  $\mu_3 = 1$  and  $\mu_0 = \mu_1 = \mu_2 = 0$ , reflecting the fact that the bottom strategy is winning for Eloise.

Finally, we consider an undetermined game:

$$u = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

yielding the following constraints:

$$\begin{aligned} \mu_0 &\geq v \\ \mu_1 + \mu_3 &\geq v \\ \mu_1 + \mu_2 &\geq v \\ \mu_2 + \mu_3 &\geq v. \end{aligned}$$

From the last three equations we derive that  $\mu_1 = \mu_2 = \mu_3$ . So  $\mu u$  is the row vector

$$[\mu_0, 2\mu_1, 2\mu_1, 2\mu_1].$$

From the first equation, it follows that  $\mu_0 = 2\mu_1$  so the minimal element in this vector is only maximized by assignments for which  $\mu_0 = 2\mu_1$ . Since we require that  $\mu$  be a probability distribution, there is only one such assignment: the one for which  $\mu_0 = 2/5$  and  $\mu_1 = 1/5$ . Accordingly the value of the game is  $2/5$ .

It is tempting to replace the inequality symbols  $\geq$  by the equality symbol  $=$ . Doing so does not affect the outcome of the latter game, but generally it is untrue that a maximizing  $\mu$  yields a vector  $\mu u$  of the form

$$[U(\mu, \tau_0), \dots, U(\mu, \tau_{n-1})]$$

of equal values. See for instance the game:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \quad (10)$$

Eloise's strategy  $\mu$  such that  $\mu_0 = \mu_1 = \mu_3 = 1/7$  and  $\mu_2 = \mu_4 = 2/7$  maximizes  $\min_{\tau}(\mu, \tau) = 3/7$ . However,  $U(\mu, \tau_2) = 4/7$ . To see that there is no maximizing  $\mu$  that yields a vector  $\mu u$  of equal values, consider the game's corresponding linear programming problem, replacing  $\geq$  by  $=$ , we get

$$\mu_0 + \mu_1 + \mu_3 = v \quad (11)$$

$$\mu_2 + \mu_3 = v \quad (12)$$

$$\mu_2 + \mu_4 = v \quad (13)$$

$$\mu_1 + \mu_2 = v \quad (14)$$

$$\mu_3 + \mu_4 = v \quad (15)$$

$$\mu_0 + \mu_4 = v. \quad (16)$$

Eqs. (12) and (13) imply  $\mu_3 = \mu_4$ . In the same vein, Eqs. (13) and (14) imply  $\mu_1 = \mu_4$ ; Eqs. (15) and (16) imply  $\mu_0 = \mu_3$ ; and Eqs. 12 and 15 imply  $\mu_2 = \mu_4$ . We conclude that  $\mu_0 = \dots = \mu_4 = 1/5$ , contradicting Eqs. (11) and (12).

### 3.2 Bounds and characterizations

For an  $m \times n$  matrix  $u$ , we let  $\text{col-min}(u)$  denote

$$\min \{ \Sigma \text{Col}^u(0), \dots, \Sigma \text{Col}^u(n-1) \},$$

and  $\text{col-argmin}(u)$  the set of indices  $0 \leq j < n$  for which

$$\Sigma \text{Col}^u(j) = \text{col-min}(u).$$

In a similar way we introduce row-max and row-argmax. We define

$$\text{Floor}(u) = \frac{\text{col-min}(u)}{m}$$

and

$$\text{Ceil}(u) = \frac{\text{row-max}(u)}{n}.$$

For instance, the matrix  $u$  in (10) has  $\text{Floor}(u) = 1/5$  and  $\text{Ceil}(u) = 3/6$ .

**Proposition 3.** *For a game  $u$ ,*

1.  $\text{Floor}(u) = \min_{\nu} U(\bar{\mu}, \nu)$ , where  $\bar{\mu}$  is Eloise's uniform strategy; and
2.  $\text{Floor}(u) \leq \mathcal{V}(u)$ .

*Proof.* Claim (1). Suppose  $u$  is an  $m \times n$  game. Eloise's strategy  $\bar{\mu}$  assigns  $1/m$  to each strategy  $0 \leq i < m$ . Multiplying  $\bar{\mu}$  with  $u$  yields:

$$[\Sigma \text{Col}^u(0)/m, \dots, \Sigma \text{Col}^u(n-1)/m].$$

Abelard picks a strategy that yields

$$\min_j U(\bar{\mu}, j) = \text{col-min}(u)/m = \text{Floor}(u)$$

for Eloise. By Eq. (9), no mixed strategy of Abelard can outperform  $j$ , given that Eloise plays  $\bar{\mu}$ :

$$\min_j U(\bar{\mu}, j) = \min_{\nu} U(\bar{\mu}, \nu).$$

Claim (2). Playing  $\bar{\mu}$  yields at least  $\text{Floor}(u)$  for Eloise, by Claim (1). So Eloise can secure at least  $\text{Floor}(u)$  in  $u$ .  $\square$

**Proposition 4.** *For a game  $u$ ,*

1.  $\text{Ceil}(u) = \max_{\mu} U(\mu, \bar{\nu})$ , where  $\bar{\nu}$  is Abelard's uniform strategy; and
2.  $\mathcal{V}(u) \leq \text{Ceil}(u)$ .

*Proof.* Analogous to the proof of Proposition 3.  $\square$

**Proposition 5.** *For a balanced game  $u$ ,*

1.  $\mathcal{V}(u) = \text{Floor}(u) = \text{Ceil}(u)$ ; and
2. the strategy profile  $(\bar{\mu}, \bar{\nu})$  is an equilibrium in  $u$ .

*Proof.* Claim (1). Suppose  $u$  is an  $m \times n$  game. By the fact that the game is column balanced it follows from Proposition 3 that the value of the game is at least

$$\text{Floor}(u) = \frac{\Sigma \text{Col}^u(0)}{m}.$$

By the fact that the game is row balanced it follows from Proposition 4 that the value of the game is at most

$$\text{Ceil}(u) = \frac{\Sigma \text{Row}^u(0)}{n}.$$

Since  $u$  is row balanced, it has precisely  $m \Sigma \text{Row}^u(0)$  entries with a 1; since it is column balanced, it has precisely  $n \Sigma \text{Col}^u(0)$  entries with a 1. Hence,  $m \Sigma \text{Row}^u(0) = n \Sigma \text{Col}^u(0)$ , and it follows that the upper and lower bounds coincide, since we have that

$$\frac{\Sigma \text{Row}^u(0)}{n} = \frac{\Sigma \text{Col}^u(0)}{m}.$$

The equality  $\mathcal{V}(u) = \text{Ceil}(u)$  can be derived similarly.

Claim (2). Observe that:

$$U(\bar{\mu}, \bar{\nu}) \leq \max_{\mu} U(\mu, \bar{\nu}) = \min_{\nu} U(\bar{\mu}, \nu) \leq U(\bar{\mu}, \bar{\nu}).$$

The equality follows from Claim (1) and Propositions 3.1 and 4.1; the inequalities follow from the definition of max and min, respectively. It follows that

$$\max_{\mu} U(\mu, \bar{\nu}) = U(\bar{\mu}, \bar{\nu}) = \min_{\nu} U(\bar{\mu}, \nu).$$

From this equality it follows that for every  $\mu$  and  $\nu$ ,

$$U(\mu, \bar{\nu}) \leq \max_{\mu} U(\mu, \bar{\nu}) = U(\bar{\mu}, \bar{\nu}) = \min_{\nu} U(\bar{\mu}, \nu) \leq U(\bar{\mu}, \nu),$$

and  $(\bar{\mu}, \bar{\nu})$  is an equilibrium of  $u$ , by definition.  $\square$

**Example 6.** Consider the  $n \times n$  matrix  $u$  with 1s on the diagonal:

$$\begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix}.$$

This matrix is obviously balanced. Whence, by Proposition 5, the value is  $1/n$ . Note that  $u$  is isomorphic to games  $\Gamma(\mathbb{M}, \phi_{\text{MP}})$  of the Matching Pennies sentence on structures  $\mathbb{M}$  with  $n$  elements.

A row submatrix  $u'$  of  $u$  is any matrix that can be obtained by deleting any number of rows from  $u$  (in any order).

**Proposition 7.** For a game  $u$ ,

$$\max_{u'} \text{Floor}(u') \leq \mathcal{V}(u),$$

where  $u'$  ranges over the nonempty row submatrices of  $u$ .

*Proof.* Suppose  $u$  is an  $m \times n$  matrix. For a row submatrix  $u'$  of  $u$  with  $m'$  rows, define the mixed strategy  $\mu$  in the game of  $u$  for which

$$\mu(i) = \begin{cases} 1/m' & \text{if Row}^u(i) \text{ is also a row in } u' \\ 0 & \text{otherwise.} \end{cases}$$

The strategy  $\mu$  plays all rows in  $u'$  with equal probability, and does not play any of the rows in  $u$  that do not sit in  $u'$ . Hence  $\mu u$  yields

$$[\Sigma \text{Col}^{u'}(0)/m', \dots, \Sigma \text{Col}^{u'}(n-1)/m'].$$

The minimal value in this vector equals  $\text{Floor}(u')$ . So Eloise can iterate through all row submatrices  $u'$ . Then, she can secure  $\text{Floor}(u')$  by playing the mixed strategy associated with a  $u'$  that maximizes  $\text{Floor}(u')$ .  $\square$

**Proposition 8.** *Let  $u'$  be a row submatrix of the game  $u$ . If  $u'$  is balanced and*

$$\text{row-max}(u) = \text{row-max}(u'),$$

*then*

1.  $\mathcal{V}(u) = \mathcal{V}(u')$ ; and
2. *the strategy profile  $(\bar{\mu}, \bar{\nu})$  of Eloise's and Abelard's uniform strategies in  $u'$  respectively, is an equilibrium in  $u$ .*

*Proof.* Claim (1). By Propositions 7 and 5.1,

$$\mathcal{V}(u') \leq \mathcal{V}(u),$$

and by Propositions 4.2,

$$\mathcal{V}(u) \leq \text{Ceil}(u).$$

Since  $u'$  is balanced, it follows from Proposition 5.1 that

$$\text{Floor}(u') = \mathcal{V}(u') = \text{Ceil}(u').$$

Since  $\text{row-max}(u) = \text{row-max}(u')$ , we have that  $\text{Ceil}(u) = \text{Ceil}(u')$ . Hence

$$\mathcal{V}(u') = \mathcal{V}(u).$$

Claim (2). By Proposition 5.2, the pair of uniform strategies  $(\bar{\mu}, \bar{\nu})$  is an equilibrium in  $u'$ , whence for every mixed strategy  $\nu$  in  $u'$ ,

$$U'(\bar{\mu}, \bar{\nu}) \leq U'(\bar{\mu}, \nu),$$

where  $U'$  is the expected utility function of  $u'$ . Since  $u'$  is a submatrix of  $u$ ,  $U'$  and  $U$  agree on every pair of mixed strategies in the domain of  $U'$ . Since  $u'$  is a *row* submatrix of  $u$ , Abelard's set of strategies in the two games coincide. Therefore, the latter inequality boils down to

$$U(\bar{\mu}, \bar{\nu}) \leq U(\bar{\mu}, \nu),$$

for every mixed strategy  $\nu$  of Abelard in  $u$ . Remark that strictly speaking, in this inequality,  $\bar{\mu}$  denotes Eloise's mixed strategy in  $u$  that is uniform in the strategies that are shared between  $u$  and  $u'$ .

If Abelard plays  $\bar{\nu}$ , Eloise can secure the maximal element in  $u\bar{\nu}$ . For the transposition of this vector write

$$[w_0, \dots, w_{m'-1}, w_{m'}, \dots, w_{m-1}],$$

assuming  $u$  is an  $m \times n$  game and  $u'$  is an  $m' \times n$  game, with  $m' \leq m$ . Since  $u'$  is balanced all its rows have the same sum, namely  $\text{row-max}(u') = \text{row-max}(u)$ . Thus,

$$\text{row-max}(u)/n = w_0 = \dots = w_{m'-1}.$$

Here we assume that the first  $m'$  rows in  $u$  constitute  $u'$ , which obviously goes without loss of generality. Furthermore, we may assume that

$$w_{m'-1} \geq w_{m'} \geq \dots \geq w_{m-1}.$$

Since  $\bar{\mu}$  only assigns non-zero probabilities to the first  $m'$  strategies, no mixed strategy  $\mu$  of Eloise in  $u$  can outperform  $\bar{\mu}$ , given that Abelard plays  $\bar{\nu}$ :

$$U(\mu, \bar{\nu}) \leq U(\bar{\mu}, \bar{\nu}).$$

It follows that  $(\bar{\mu}, \bar{\nu})$  is an equilibrium in  $u$ . □

## 4 Applications

We give two applications of the tools developed to equilibrium semantics.

### 4.1 Birthday problem

Considered is a party attended by  $m$  persons. What is the probability that there is a pair of individuals that have the same birthday? A straightforward combinatorial argument shows that the probability exceeds 50 per cent when  $m > 20$ .

The “birthday problem” can be redefined in terms of drawing  $m$  balls (number of guests) from an urn of  $n$  balls (number of birthdays) with replacement. We are interested in the odds that we draw the same ball twice.

Given the first ball  $b_0$ , the probability that the second ball  $b_1$  is not equal to  $b_0$  is

$$\frac{n-1}{n}.$$

Similarly, given  $i$  distinct balls  $b_0, \dots, b_{i-1}$ , the probability that the next ball is not among the balls drawn earlier is

$$\left(\frac{n}{n}\right) \left(\frac{n-1}{n}\right) \left(\frac{n-2}{n}\right) \dots \left(\frac{n-i}{n}\right).$$

It follows that the odds that  $b_0, \dots, b_{m-1}$  are all distinct is

$$\frac{n!}{n^m (n-m)!}. \tag{17}$$

We define the process of randomly drawing  $m$  balls from the urn in IF logic. Consider the IF sentence

$$\phi_m = \forall x_0 \dots (\forall x_{m-1}/X_{m-1})(\exists x_m/X_m) \dots (\exists x_{2m-1}/X_{2m-1})\psi_m$$

where  $X_k = \{x_0, \dots, x_{k-1}\}$  and

$$\psi_m = \bigvee_{0 \leq i < m} \bigvee_{i < j < m} (x_i + x_{i+m}) = (x_j + x_{j+m}),$$

in which the addition operator is defined as  $a_k + a_l = a_{k+l \bmod n}$  assuming that the  $n$  objects in the domain at hand are labeled  $a_1, \dots, a_{n-1}$ . In an extensive game of  $\phi_m$ , Abelard and Eloise pick  $m$  objects each. Abelard's first object  $a_0$  is added to Eloise's first object  $a_m$ , and so on for the other  $m-1$  objects. Since Eloise does not know any of Abelard's choices, the object  $b_i = a_i + a_{m+i}$  is effectively chosen at random. Eloise wins if there is a pair of sums  $b_i = b_j$  with  $i < j$ ; otherwise Abelard wins.

**Proposition 9.** *The probability that a random sample of  $m$  elements from a set of  $n$  elements (with replacement) contains at least one pair of duplicates is  $\mathcal{V}(\mathbb{M}, \phi_m)$  for any structure  $\mathbb{M}$  of size  $n$  in which the addition operator is defined as above.*

*Proof.* Both Abelard and Eloise have  $n^m$  choices for their respective quantifiers. Then, Eloise has two disjunction choices knowing Abelard's and her own moves (or more if we permit ourselves only binary disjunctions). Given this knowledge, she has an "optimal substrategy": chose the first disjunct that holds with respect to the chosen objects, if such a disjunct exists; otherwise, select an arbitrary disjunct. It is clear that this strategy outperforms or is equivalent to any other substrategy she may have, given the objects selected for the objects. It has been shown that we can remove such "weakly dominated" and "payoff equivalent" strategies from the strategic game, without affecting the game's value [10, Proposition 7.25].

Thus we can focus on the game that is the result of eliminating weakly dominated and payoff equivalent strategies. In this reduced game, each of Abelard's and Eloise's strategies corresponds to an ordered series of  $n$  objects from  $M$ . So, each player has  $n^m$  strategies. Consider any strategy  $(a_0, \dots, a_{m-1})$  of Abelard. Let us count the number of strategies  $(a_m, \dots, a_{2m-1})$  of Eloise against which Abelard's strategy results in a loss for Eloise. The object  $a_m$  can be chosen in any way we want, yielding  $n$  choices. Write  $b_i$  for  $a_i + a_{m+i}$ . Given a series of  $i$  distinct objects  $b_0, \dots, b_{i-1}$ , there are  $n-i$  objects  $a_{m+i}$  for which

$$a_i + a_{m+i} \notin \{b_0, \dots, b_{i-1}\}.$$

So every strategy of Abelard loses against  $n(n-1)(n-2) \dots (n-m) = n!/(n-m)!$  strategies of Eloise, and wins against

$$n^m - \frac{n!}{(n-m)!} \quad (18)$$

strategies. The strategy of Abelard was chosen without loss of generality; it follows that  $u$  is row balanced and that the value (18) equals  $n^m -$



$\text{col-min}(u)$ , where  $u$  is the matrix of the reduced strategic game of  $\phi_m$  on  $\mathbb{M}$ . Since  $u$  has  $n^m$  columns,

$$\text{Floor}(u) = \frac{\text{col-min}(u)}{n^m} = \frac{n!}{n^m(n-m)!} = (17).$$

A symmetric argument shows that  $u$  is also row balanced. By Proposition 5 it follows that the value of  $\phi_m$  on  $\mathbb{M}$  is (17).  $\square$

What is at stake in the birthday problem is the number of *pairs* of party goers  $m(m-1)/2$ , which is quadratic in  $m$ . This is reflected in the IF sentence  $\phi_m$ , which has  $2m$  quantifiers to simulate the random selection of  $m$  objects. The quantifier-free prefix  $\psi_m$  has  $m(m-1)/2$  disjuncts, one for each pair of distinct party goers.

## 4.2 Universal hashing

In this section we use IF logic to describe the game theory behind *universal hashing*, a notion from computer science. Hashing functions are used to map an unknown set  $S$  from a set of objects  $U$  called *keys*, to a set of *hash values*  $V$ . If we have a linear order on  $V$ , then we can use a hash function to store the elements from  $S$  in a hash table, which allows for binary search.

For instance, we can think of  $U$  as the collection of all finite strings with at most 100 characters,  $S$  as the set of Dutch names, and  $V$  as some range of integers in an administration system. Surely, we do not want to reserve as many integers as there are elements in  $U$ ; a hash function helps us transfer an arbitrary key from  $U$  to a hash value in  $V$ .

By the pigeon hole principle, if  $S$  has more elements than  $V$ , for every hash function, there is a pair of keys  $k, l \in U$  that are mapped to the same hash value. Such a pair of objects is said to *collide*. Collision handling is typically resource intensive, for which reason we want to select a hash function that minimizes the expected number of collisions not knowing the set  $S$  of keys that will actually materialize. The following fragment explains hashing as a game.

“If a malicious adversary chooses the keys to be hashed by some fixed hash function, then he can choose  $n$  keys that all hash to the same slot, yielding an average retrieval time [that is linear in  $n$ ]. Any fixed hash function is vulnerable to such terrible worst-case behavior; the only effective way to improve the situation is to choose the hash function *randomly* in a way that is *independent* of the keys that are actually going to be stored. This approach, called *universal hashing*, can yield provably good performance on average, no matter what keys are chosen by the adversary.

The main idea behind universal hashing is to select the hash function at random from a carefully designed class of functions at the beginning of execution. [...] Poor performance occurs only when the compiler chooses a random hash function that causes the set of identifiers to hash poorly, but the probability

of this situation occurring is small and is the same for any set of identifiers of the same size.” [2, pp. 232–3]

We will work on *hash structures*

$$\mathbb{M} = (M, U^{\mathbb{M}}, (f_i^{\mathbb{M}})_{0 \leq i < n}),$$

where  $U^{\mathbb{M}} \subseteq M$  are the keys,  $M - U^{\mathbb{M}}$  the hash values,  $(f_i^{\mathbb{M}})_i$  is the series of all functions from  $U^{\mathbb{M}}$  to  $M - U^{\mathbb{M}}$  and  $i$  is an injective indexing of thereof. The assumption that a hash structure records all possible hash functions with respect to the set of keys and values at hand is very strong. We will return to this assumption before we leave this section.

The game dynamics described in the first part of the first paragraph are captured by:

$$\phi_H = \bigvee_i \forall x \forall y \left[ (U(x) \wedge U(y) \wedge x \neq y) \rightarrow f_i(x) \neq f_i(y) \right],$$

in which the operator  $\bigvee_i$  is object language.

In a game of  $\phi_H$  on a hash structure  $\mathbb{M}$ , triggered by  $\bigvee_i$  Eloise chooses the index  $i$  of the hash function  $f_i^{\mathbb{M}}$ . Then, Abelard in the capacity of malicious adversary chooses two keys for  $x$  and  $y$ . If they collide with respect to  $f_i^{\mathbb{M}}$ , Abelard wins. As we pointed out above, by the pigeonhole principle, Abelard has a winning strategy whenever  $|U| > |V|$ .

As explained in the remainder of the quotation, in the universal hashing scenario, Eloise tries to confuse Abelard by drawing her hash function at random. We will show that the optimal way to randomly select a hash function coincides with Eloise’s equilibrium strategy in the game described by

$$\phi_{UH} = \bigvee_i (\forall x/i)(\forall y/i) \left[ (U(x) \wedge U(y) \wedge x \neq y) \rightarrow f_i(x) \neq f_i(y) \right].$$

Assume  $U = \{k_0, \dots, k_{n-1}\}$  and  $V = \{0, \dots, m-1\}$ . For a function  $f : U \rightarrow V$ , let  $\mathcal{P}_f$  be the set of its pre-images:

$$\mathcal{P}_f = \{f^{-1}(v) : v \in V\}.$$

The *degree* of a function  $f$  is the difference between the sizes of the largest and smallest pre-image in  $\mathcal{P}_f$ :

$$\max \{|P| : P \in \mathcal{P}_f\} - \min \{|P| : P \in \mathcal{P}_f\}.$$

For every  $U$  and  $V$  there is a function  $f : U \rightarrow V$  of degree (at most) 1, see for instance the function

$$f(k_i) = i \bmod m.$$

This function has in fact degree 0 whenever  $n \bmod m = 0$ .

In the context of the game  $\Gamma(\mathbb{M}, \phi_{UH})$ ,  $S_d$  denotes the set of strategies of Eloise that pick indices  $i$  for which  $f_i^{\mathbb{M}}$  has degree  $d$ . Each strategy of Abelard corresponds to the pair of keys  $(k, l)$  it assigns to  $x$  and  $y$ . We write  $T^*$  for the set of strategies of Abelard that assign distinct keys to  $x$  and  $y$ .

**Proposition 10.** *Let  $d = \min\{1, n \bmod m\}$  and  $S^* = S_d$ . The pair of uniform strategies  $(\bar{\mu}, \bar{\nu})$  over  $S^*$  and  $T^*$  respectively is an equilibrium in  $\Gamma = \Gamma(\mathbb{M}, \phi_{UH})$ .*

*Proof.* Every strategy of Abelard that does not sit in  $T^*$  is losing for Abelard, and therefore weakly dominated by every strategy in  $T^*$ . Whence, we may discard these dominated strategies from our analysis, see [10, Chapter 7].  $T^*$  contains  $n^2 - n$  strategies.

We consider a function  $\lambda$  on the set of functions of type  $U \rightarrow V$ . Let  $f$  be one particular function of this type. Write  $i_{\max}^f$  for a value with largest pre-image:

$$i_{\max}^f = \operatorname{argmax}_i \{|f(i)^{-1}|\}.$$

Let  $k^*$  be any element in  $f(i_{\max}^f)^{-1}$ . Similarly, write  $i_{\min}^f$  for a value with smallest pre-image:

$$i_{\min}^f = \operatorname{argmin}_i \{|f(i)^{-1}|\}.$$

Then,  $\lambda$  sends  $f$  to the function  $\lambda(f)$  for which

$$\lambda(f)(k) = \begin{cases} i_{\min}^f & \text{if } k = k^* \\ f(k) & \text{otherwise.} \end{cases}$$

If a collision occurs, it is more likely to happen between keys that are sent to  $i_{\max}^f$  than to keys sent to  $i_{\min}^f$ . The operator  $\lambda$  levels the probability that a collision occurs at  $i_{\max}^f$  and the probability that one occurs at  $i_{\min}^f$ . We will see that it also decreases the likelihood of a collision appearing in the first place.

Write  $\sigma$  and  $\sigma'$  for Eloise's strategies in  $\Gamma$  that pick the indices of  $f$  and  $f' = \lambda(f)$ , respectively. We show that  $\sigma$  loses against more strategies of Abelard than  $\sigma'$ . Eloise's strategy  $\sigma$  loses against Abelard's strategies in

$$L_\sigma = \bigcup_{P \in \mathcal{P}_f} L_P.$$

where

$$L_P = \{(k, l) \in T^* : k, l \in P\}.$$

Similarly,  $\sigma'$  loses against the strategies in  $L_{\sigma'} = \bigcup_{P \in \mathcal{P}_{f'}} L_P$ . To show that  $|L_\sigma| > |L_{\sigma'}|$ , it suffices to show that

$$|L_{f(i_{\max}^f)^{-1}}| + |L_{f(i_{\min}^f)^{-1}}| > |L_{f'(i_{\max}^f)^{-1}}| + |L_{f'(i_{\min}^f)^{-1}}|, \quad (19)$$

because the other pre-images are shared between  $f$  and  $f'$ . For a pre-image  $P$  of size  $z$ ,  $L_P$  contains  $z(z-1)$  elements. Whence, if  $f(i_{\min}^f)^{-1}$  contains  $x$  elements,

$$\begin{aligned} |L_{f(i_{\max}^f)^{-1}}| &= x(x-1) \\ |L_{f'(i_{\max}^f)^{-1}}| &= (x-1)(x-2). \end{aligned}$$

Likewise, if  $f(i_{\min}^f)^{-1}$  contains  $y$  elements,

$$\begin{aligned} |L_{f(i_{\min}^f)^{-1}}| &= y(y-1) \\ |L_{f'(i_{\min}^f)^{-1}}| &= (y+1)y. \end{aligned}$$

Hence, Eq. (19) reduces to

$$x(x-1) + y(y-1) > (x-1)(x-2) + (y+1)y,$$

which is the case if  $x > y + 1$ .

We leave it as an exercise to the reader to verify that for any function  $f$  of degree  $d' > 1$ , there is a finite series

$$f, \lambda(f), \lambda(\lambda(f)), \dots, \lambda(\dots \lambda(\lambda(f)) \dots)$$

of which the final element has degree  $d' - 1$ . Thus, iterative application of  $\lambda$  ultimately yields a function with degree  $d$ . As we have just shown above, every application of  $\lambda$  yields a hash function that further reduces the number of strategies against which the strategy loses that picks the index of that hash function. If we reach a function with degree  $d$ , applying  $\lambda$  no longer reduces this number. It can further be checked that as long as  $\lambda$  can be applied,  $x > y + 1$ .

It is easy to see that every two functions with degree  $d$  suffer from an equal number of collisions. Let  $\Gamma^*$  be the subgame of  $\Gamma$  induced by  $S^*$  and  $T^*$ , that is,  $\Gamma^*$  is of the form  $(S^*, T^*, u^*)$  where  $u^*(\sigma, \tau) = u(\sigma, \tau)$ , for any  $\sigma \in S^*$  and  $\tau \in T^*$ .

Our  $\lambda$ -argument showed that  $\text{row-max}(u^*) = \text{row-max}(u)$ . Since every two functions of degree  $d$  suffer from the same number of collisions,  $u^*$  is row balanced. It is easy to see that  $u^*$  is also column balanced. We apply Proposition 8.2 to infer that  $(\bar{\mu}, \bar{\nu})$  is an equilibrium in  $\Gamma$ .  $\square$

We have seen in the section on the birthday problem, Section 4.1, that we can simulate drawing random objects, but we were incapable of extending this method to drawing random functions. It appears to us that if we have a means to express randomization over functions, we can utilize this mechanism to express universal hashing without assuming structures that carry all possible hash structures.

If it turns out that IF logic can express random functions, or if it turns out that it cannot, we may be able to use this to prove new upper or lower bounds on the expressive power of IF under equilibrium semantics. In fact, if the former is the case — i.e., IF logic can express random functions — it would be most interesting to see if it has natural fragments that coincide with randomized complexity classes in the style of Fagin’s Theorem, which showed that second-order existential logic coincides with the complexity class NP [4].

## 5 Acknowledgements

We gratefully acknowledge Fausto Barbero for careful proofreading.

## References

- [1] A. Blass and Y. Gurevich. Henkin quantifiers and complete problems. *Annals of Pure and Applied Logic*, 32:1–16, 1986.

- [2] T. Cormen, C. Leiserson, R. Rivest, and C. Stein. *Introduction to Algorithms*. McGraw-Hill, second edition, 2003.
- [3] F. Dechesne. *Game, Set, Maths: Formal investigations into logic with imperfect information*. PhD thesis, Tilburg University, Tilburg, 2005.
- [4] R. Fagin. Generalized first-order spectra and polynomial-time recognizable sets. In R. M. Karp, editor, *SIAM-AMS Proceedings, Complexity of Computation*, volume 7, pages 43–73, 1974.
- [5] P. Galliani. Game values and equilibria for undetermined sentences of dependence logic. Master’s thesis. Master of Logic Series 2008-08, University of Amsterdam, Amsterdam, 2008.
- [6] P. Galliani and A. L. Mann. Lottery semantics: A compositional semantics for probabilistic first-order logic with imperfect information. *Studia Logica*, in press.
- [7] J. Hintikka. *Logic, Language Games and Information*. Clarendon, Oxford, 1973.
- [8] J. Hintikka. *Principles of Mathematics Revisited*. Cambridge University Press, Cambridge, UK, 1996.
- [9] J. Hintikka and G. Sandu. Informational independence as a semantic phenomenon. In J. E. Fenstad et al., editor, *Logic, Methodology and Philosophy of Science*, volume 8, pages 571–589. Elsevier, Amsterdam, 1989.
- [10] A. L. Mann, G. Sandu, and M. Sevenster. *Independence-Friendly Logic: A Game-Theoretic Approach*. Cambridge University Press, 2011.
- [11] John Nash. Non-cooperative games. *Annals of Mathematics*, 54:286–295, 1951.
- [12] T. E. S. Raghavan. Zero-sum two person games. In R. J. Aumann and S. Hart, editors, *Handbook of Game Theory with Economic Applications*, volume 2, pages 736–759. Elsevier, Amsterdam, 1994.
- [13] M. Sevenster. *Branches of Imperfect Information: Logic, Games, and Computation*. PhD thesis, University of Amsterdam, Amsterdam, 2006.
- [14] M. Sevenster and G. Sandu. Equilibrium semantics of languages of imperfect information. *Annals of Pure and Applied Logic*, 161:618–631, 2010.
- [15] J. von Neumann. Zur Theorie der Gesellschaftsspiele. *Mathematische Annalen*, 100:295–320, 1928.
- [16] Ludwig Wittgenstein. *Philosophical Investigations*. Basil Blackwell, Oxford, 1958. Translated by G. E. M. Anscombe.